GIBSON DUNN

Judith Alison Lee is a partner at Gibson, Dunn & Crutcher LLP. She can be contacted on +1 (202) 887 3591 or by email: jalee@gibsondunn.com.

EXPERT BRIEFING February 2022

US Commerce Department takes more action against Chinese companies

BY JUDITH ALISON LEE

In recent months, the US Commerce Department has been on the front line of the Biden administration's efforts to pressure China in the areas of national security, trade and export controls.

New proposed regulation on connected software applications

On 26 November 2021, the Commerce Department published a notice of proposed rulemaking which sought to amend the January Supply Chain Rule to provide for additional criteria that the secretary of commerce "may consider specifically when determining whether ICTS transactions – defined in the Supply Chain Rule as those that involve connected software applications which present an undue or unacceptable risk". The notice revises the definition of ICTS to include "connected software applications" and adds a definition of "connected software application" that is consistent with president Biden's Executive Order 14034.

The new criteria proposed in the notice are: (i) ownership, control or management by persons who support a foreign adversary's military, intelligence or proliferation activities; (ii) use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data; (iii) ownership, control or management of connected software applications by persons subject to coercion or cooption by a foreign adversary; (iv) ownership, control or management of connected software applications by persons involved in malicious cyber activities; (v) a lack of thorough and reliable third-party auditing of connected software applications; (vi) the scope and sensitivity of the data collected; (vii) the number and sensitivity of the users of the connected software application; and (viii) the extent to which identified risks have been or can be addressed by independently verifiable measures.

The Commerce Department noted that it is interested in the public's views on the additional criteria for connected software applications, including whether they should be applied to all ICTS transaction reviews, whether there are other criteria that should be

applied and how the secretary should apply the criteria to ICTS transactions involving connected software applications.

Specifically, the Commerce Department posed the following questions.

First, should "ownership, control or management" be understood to include both continuous control and management and sporadic control and management (e.g., when a third-party must be temporally granted access to apply updates, upgrades and patches, etc.), or should this phrase be further clarified?

Second, should the Commerce Department add a criterion such as whether the software has any embedded outgoing network calls or web server references, regardless of the ownership, control or management of the software?

Third, how should the Commerce Department define the terms "reliable third-party" and "independently verifiable measures?"

Fourth, is the reference to "third-party auditing of connected software applications" sufficiently clear or does it need further definition?

Fifth, should the requirement to audit applications be revised to make clear that auditing is a continuous process through the development and deployment lifecycle of the application?

Finally, should the requirement to audit applications be understood to refer only to source code examination and verification, or would it also include monitoring of logs or other data that the application collects?

The "ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary" criterion, among others, is likely to be used as a basis to challenge software created and managed by Chinese technology companies, as China is one of the six identified "foreign adversaries". In response, Chinese companies will likely have to demonstrate "independently verifiable measures" to mitigate the risks identified by the US government.

There may be further changes, revisions and additions to the proposed evaluation criteria based on the public's comments, and the details of certain key concepts, including what "independently verifiable measures" would entail, are unclear at the moment. However, initiatives such as requiring a software bill of materials (SBOM), proposed by the National Telecommunications and Information Administration (NTIA), may inform and shape the criteria for evaluating software under the ICTS supply chain controls regime.

According to the NTIA, an SBOM is a "formal record containing the details and supply chain relationships of various components used in building software". These components, including libraries and modules, can be open source or proprietary, free or paid, and the data can be widely available or access restricted. In a notice issued in June 2021, the NTIA proposed a definition of the minimum elements of an SBOM that "builds on three broad, inter-related areas: data fields, operational considerations, and support for automation". It is possible, for example, for the Commerce Department to allow foreign technology companies to submit an SBOM for its software products for ICTS transaction review.

CFIUS implications of the notice of proposed rulemaking

The Committee on Foreign Investment in the United States (CFIUS) regime operates in parallel with the ICTS regime. CFIUS is an inter-agency federal government committee authorised to review the national security implications associated with foreign acquisitions of or investments in US businesses and certain transactions involving US real estate. While the ICTS regime may be similar in many respects to the CFIUS regime – in that they are both concerned with national security risks in transactions involving certain US businesses – they each cover different spheres of activities and have a different (although overlapping) set of considerations.

For example, The ICTS regime covers a broader universe of transactions, including individual commercial sales, while the CFIUS regime only covers acquisitions and investments. The Commerce Department has further clarified that the ICTS Rule does not apply to transactions that CFIUS is actively reviewing or has reviewed. Moreover, the ICTS Rule allows the Commerce Department to prohibit or restrict transactions, while a CFIUS review involves the interests of nine permanent agencies, among which the Commerce Department is a member. Thus, although the recent notice and its proposed criteria may provide a helpful insight into what the Commerce Department would consider in evaluating the national security risks within the ICTS industry, it does not directly translate to a change in the way that CFIUS reviews would be conducted.

Additionally, various risk factors identified in the notice's amendment to section 7.103 are factors that CFIUS already considers in making a national security risk evaluation. Of note, CFIUS already considers whether the US business being acquired or invested in deals with sensitive personal data. The 2018 Foreign Investment Risk Review and Modernization Act (FIRRMA) expanded the scope of transactions subject to the Committee's review to include non-controlling but non-passive foreign investments in US businesses involved in critical technologies, critical infrastructure or sensitive personal data of US citizens.

FIRRMA provided additional factors for CFIUS review, including access to "personally identifiable information, genetic information, or other sensitive data on United States citizens ... that may exploit that information in a manner that threatens national security". Since FIRRMA, CFIUS has in fact emphasised the protection of US personal information from foreign entities in a number of its recent decisions. As such, the personal data-related factors – the use of sensitive personal data, the scope and sensitivity of the data collected, and the number and sensitivity of the users – are likely to continue being an important part of CFIUS determinations.

Twenty-seven entities and individuals added to the Commerce Department's Entity List

On 26 November 2021, the Commerce Department's Bureau of Industry and Security published a Final Rule adding 27 foreign entities and individuals to the Entity List for engaging in activities that are contrary to the national security or foreign policy interests of the US. Several Chinese technology companies were added to the list in order to "prevent U.S. emerging technologies from being used for the PRC's quantum computing efforts that support

military applications, such as counter-stealth and counter-submarine applications, and the ability to break encryption or develop unbreakable encryption".

The Commerce Department stated that the Chinese technology companies added to the Entity List "support the military modernisation of the People's Liberation Army and/or acquire and attempt to acquire U.S. origin-items in support of military applications".

In 2022, the Biden administration will continue its whole-of-government approach to countering China's growing influence. Watch the Commerce Department in particular for the latest developments. ■